

Document Code No.: ITG-P-09-03-01

Title: King County Data Center Policy

Affected Agencies:

Authorities: KCC 2A.380.070

Keywords: Sabey, Data Center, Cable, Rack, PDU, Cabling, MDF, Access, Infrastructure

Sponsoring Agency: Department of Information Technology

Chief Information Officer signature:

Date signed and effective: 10/17/2018

926AF9FCB611466...



King County

I. Purpose:

This policy establishes the principles and parameters for the operational, administrative, safety and security practices for King County Data Center.

II. Applicability and Audience

This policy applies to the King County Data Center and all information assets therein.

[Note: IT Governance Policies apply to the Executive Branch. Applicable to independently elected agencies as baseline policy requirements.]

III. Definitions

- A. **Cable Management:** The installation and maintenance of the King County Data Center's structured cabling plan in adherence to established standards.
- B. **MDF:** The Main Distribution Frame (MDF) is a central location where external terminates and interconnects with the facilities Intermediate Distribution Frames (IDF) to provide connectivity.
- C. **Organization:** Every County office, every officer, every institution' whether educational, correctional or other; and every department, division, board, and commission.
- D. **Rack Management:** The management of the King County Data Center equipment racks, not limited to the placement of devices, power, cooling, weight, access requirements, and functional alignment.
- E. **PDU:** Power Distribution Unit
- F. **Physical infrastructure:** The foundation or framework that supports a system or organization. Information technology infrastructure is composed of physical and virtual resources that support the flow, storage, processing and analysis of data.
- G. **Structured cabling:** Complete system of cabling and associated hardware, which provides a comprehensive telecommunications infrastructure. This infrastructure serves a wide range of uses, such as to provide telephone service or transmit data through a computer network.
- H. **Workforce Member:** Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide services to King County.
- I. **Sabey:** Sabey is used to refer to the King County Data Center located in Tukwila. The name is in reference to the entity who owns the facility and whom King County leases

space to house the King County Data Center. King County must adhere to all of Sabey's security policies

IV. Policy

A. Responsibilities:

- a. The King County CIO and their appointed designee, is responsible for the physical security of King County's Data Center facilities.
- b. KCIT Production Operations is responsible for the management of the King County Data Center and the assets therein.

B. Access to the King County Data Center:

- a. All access will adhere to Sabey Data Center's security requirements, including signing confidentiality agreements
- b. Unescorted access must be pre-authorized with approved documented business need
- c. Unescorted access may not exceed 12 months in duration. Unescorted access may be extended with the re-submission of approved documented business need up to 1 month prior to access expiration.
- d. All access must remain in active state and is subject to termination at anytime
- e. Visitors, including vendors, must be pre-authorized and escorted.
- f. All persons entering and exiting the King County Data Center, with the exception of KCIT Production Operations staff, are required to sign the Data Center access log
- g. MDF access is limited to KCIT Production Operations staff and must be pre-authorized 24 hours in advance.

C. Inventory Control:

- a. KCIT Production Operations is responsible for the tracking of all King County Data Center assets.
- b. All changes to King County Data Center inventory requires advanced notification to KCIT Production Operations and submission of a Data Center Change Request (DCCR)

D. Change Management: Changes within the King County Data Center must follow the KCIT Change Management process and adhere to Sabey Data Centers change management process.

E. Physical Infrastructure: KCIT Production Operations is responsible for structured cabling, rack management, Power Distribution Units (PDU) and power connection in the King County Data Center.

F. Equipment must adhere to KCIT enterprise standards.

V. Implementation Plan

- A. This policy becomes effective for Executive Branch agencies on the date that it is signed by the County Chief Information Officer. KCIT Production Operations is responsible for implementation of this policy.
- B. King County Departments and Agencies are responsible for communicating this policy to the management structure within their respective agencies and other appropriate parties

VI. Maintenance

- A. This policy will be maintained by KCIT Production Operations
- B. This policy will automatically expire five (5) years after its effective date. A new, revised, or renewed policy will be initiated by King County Information Technology prior to the expiration date.

VII. Consequences for Noncompliance

Failure to comply will result in revocation of unescorted access privilege or access to the data center whichever is applicable.

VIII. Appendices: [Note: List Appendices using formal titles.]

NIST SP 800-14, Sept 1996: Generally Accepted Principles and Practices for Securing Information Technology Systems

NIST SP 800-53 R4, April 2013: Security and Privacy Controls for Federal Information Systems and Organizations

ISO/IEC 27002:2013: Information Technology – Security Techniques – Code of Practice for Information Security Controls